

**Module Title NETWORK SECURITY AND CRYPTOGRAPHY**

**Assignment Title Smith and Jones Auctions**

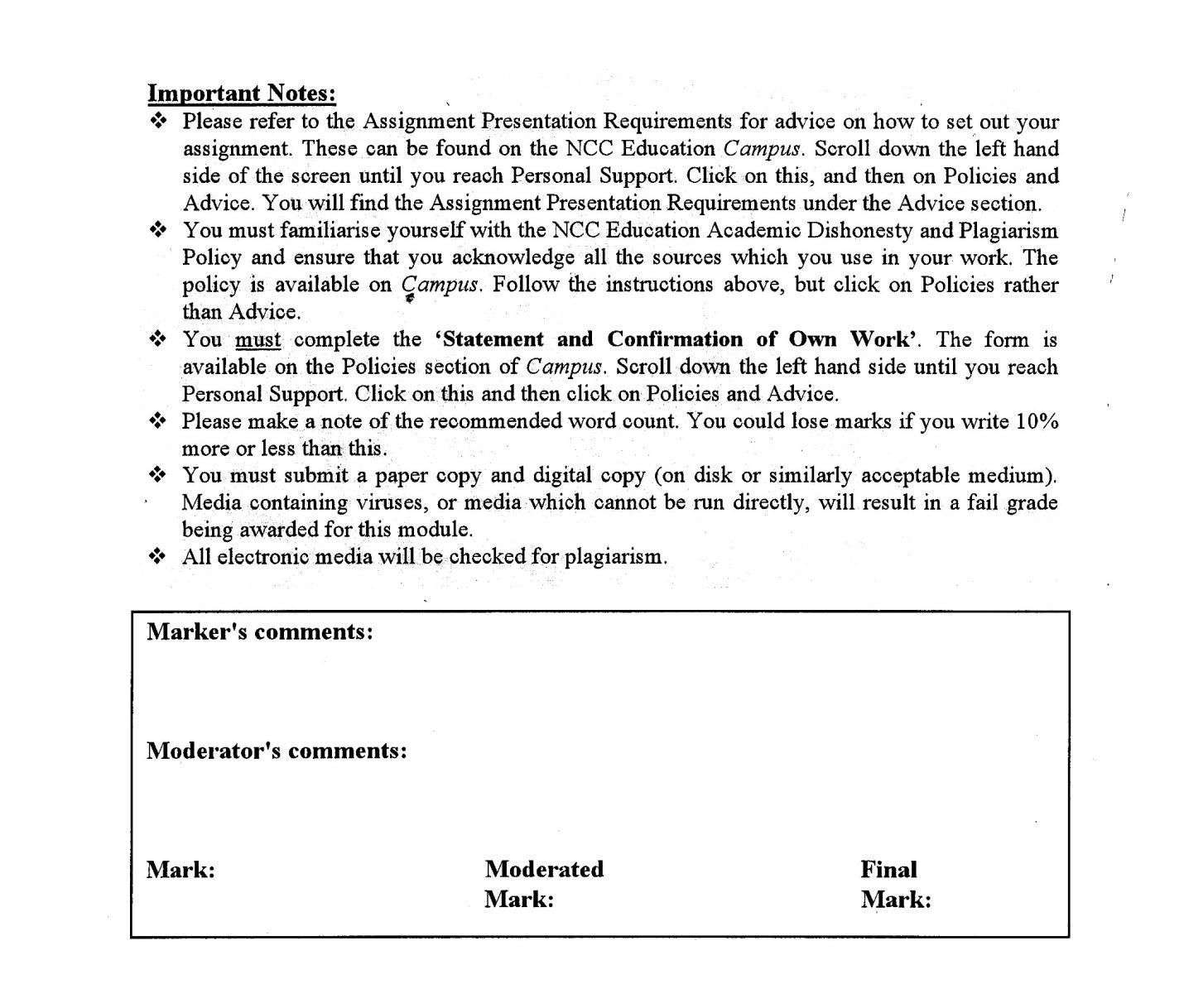
**Examination Cycle Summer 2020**

**Candidate Name LIN KHANT KO**

**Candidate No** **00183578**

**Centre Name KMD Computer Centre (Yangon)**

**Submission Date: 31st March 2020**





**Statement and Confirmation of Own Work**

**Programmed/Qualification name: Level 5 Diploma in Computing IT**

*All NCC Education assessed assignments submitted by students must have this statement as the cover page or it will not be accepted for marking. Please ensure that this statement is either firmly attached to the cover of the assignment or electronically inserted into the front of the assignment.*

**Student declaration**

I have read and understood NCC Education’s Policy on Academic Dishonesty and Plagiarism.

I can confirm the following details:

**Student ID/Registration number:**

**Name :**

**Centre Name : KMD Computer Centre (Yangon)**

**Module Name : NETWORK SECURITY AND CRYPTOGRAPHY**

**Module Leader : HEIN SI THU NYUNT**

**Number of words : 3471 Words**

I confirm that this is my own work and that I have not plagiarized any part of it. I have also noted the assessment criteria and pass mark for assignments.

**Due Date : 31st March 2020**

**Student Signature : WAI**

**Submitted Date : 31st March 2020**

Table of Contents

[Introduction 4](#_Toc37335880)

[Task 1 (Risk Assessment) 6](#_Toc37335881)

[(a) 5 Most Important Electronically Held Information 6](#_Toc37335882)

[Bidding Side Information 6](#_Toc37335883)

[Personal Information 6](#_Toc37335884)

[Email Information 6](#_Toc37335885)

[Employee Data 6](#_Toc37335886)

[Side Information 6](#_Toc37335887)

[(b) Main Security Thread 7](#_Toc37335888)

[(1) Bidding Side Information 7](#_Toc37335889)

[(2) Personal Information 7](#_Toc37335890)

[(3) Email data 7](#_Toc37335891)

[(4) Employee Data 7](#_Toc37335892)

[(5) Side Information 8](#_Toc37335893)

[(c) Likelihood and Impact 9](#_Toc37335894)

[(1) Bidding Side Information 9](#_Toc37335895)

[(2) Personal Information 9](#_Toc37335896)

[(3) Email Data 9](#_Toc37335897)

[(4) Employee Data 10](#_Toc37335898)

[(5) Side Information 10](#_Toc37335899)

[(d) Risk Matrix 10](#_Toc37335900)

[(1) Bidding Side Information 10](#_Toc37335901)

[(2) Personal Information 11](#_Toc37335902)

[(3) Email Data 11](#_Toc37335903)

[(4) Employee Data 11](#_Toc37335904)

[(5) Side Information 12](#_Toc37335905)

[Task (2) Controlling the Risk 14](#_Toc37335906)

[(a) Threats 14](#_Toc37335907)

[(1) Server Failure 14](#_Toc37335908)

[(2) Employee Thief 14](#_Toc37335909)

[(3) Environmental Risk 14](#_Toc37335910)

[(4) Hacked 15](#_Toc37335911)

[(5) Malware or Ransomware(Spyware) 15](#_Toc37335912)

[(6) DDOS Attack 15](#_Toc37335913)

[(7) Phishing 16](#_Toc37335914)

[(8) SQL Injection 16](#_Toc37335915)

[(9) Man-in-the-Middle-Attack 16](#_Toc37335916)

[(10) Rootkit 16](#_Toc37335917)

[(b) Encryption and Protocol 17](#_Toc37335918)

[Task (3) Setting up the VPN 19](#_Toc37335919)

[(a) Intranet and Extranet 19](#_Toc37335920)

[Difference of Intranet and Extranet 19](#_Toc37335921)

[**Intranet** 19](#_Toc37335922)

[**Extranet** 19](#_Toc37335923)

[Benefit of Intranet 19](#_Toc37335924)

[Benefit of Extranet 19](#_Toc37335925)

[Recommendation 19](#_Toc37335926)

[(b) Network Diagram 21](#_Toc37335927)

[(c) Rule of Firewall 22](#_Toc37335928)

[VPN Security Feature Lists 22](#_Toc37335929)

[Why Firewall needed? 22](#_Toc37335930)

[Rule of Firewall 22](#_Toc37335931)

[Task (4) Maintaining Security 25](#_Toc37335932)

[Task (5) 27](#_Toc37335933)

[(a) Problem and Solving 27](#_Toc37335934)

[(b) When I start again 27](#_Toc37335935)

# Introduction

This is about the world’s largest industrial auctioneer and they conduct the hundreds of live unreserved public actions of used heavy equipment, trucks and industrial component. Their auction take place in their auction site. Their side is more than 60 in North America, Europe, the middle each, Asia and Australia.

Task 1

Risk Assessment

# Task 1 (Risk Assessment)

## 5 Most Important Electronically Held Information

* Bidding Side Information
* Personal Information
* Email data
* Employee Data
* E-Auction Side Information

### Bidding Side Information

Bidding Side Information means all about information or complication of information related to a business, procedures, techniques and methods. Bidding Side Information is used to plan and operate the organization. Bidding Side Information can be store in the database.

(Anon., n.d.) (Anon., n.d.)

### Personal Information

Personal information include name, contact information, payment card information, and email address and more. Personal information is important because there are law and regulation that require business to meet sure standard when it comes to storing and protecting personal information.

(Anon., n.d.)

### Email Information

Email information means non-public information, business-related-information. It refers to any information that a business or individual wishes not to make public. Every business owners is trying to protect their knowledge, information, product from leaking into another.

(Anon., n.d.)

### Employee Data

Employee data is similar to customer information. It contain employee name, social security number. And they may have their banking information, username and password and data associated with a credentialing process.

(Anon., n.d.)

### E-Auction Side Information

In the E-Auction Side Information, it contain two types of sides. One is a place where take place an auction side and the second is their auction website.

## Main Security Thread

### Bidding Side Information

|  |  |  |
| --- | --- | --- |
| Asset | Threats | CIA? |
| E.g. Bidding Side Information | |  | | --- | | Employee Thief | | Server Failure | | Environmental risk | | Hacked | | Spyware | | DDOS Attack | | Phishing | | SQL Injection | | Man-in-the-Middle-Attack | | |  | | --- | | C,A | | I,A | | I | | C,A | | C,A | | I | | C,I | | C,I | | C,A | |

### Personal Information

|  |  |  |
| --- | --- | --- |
| Asset | Threats | CIA? |
| E.g. Personal Information | |  | | --- | | Server Failure | | Malware or Ransomware | | Social Media Attack | | Employee Thief | | Mobile Malware | | Computer Virus | | Phishing | | SQL Injection | | Man-in-the-Middle-Attack | | |  | | --- | | I,A | | C,A | | C | | C,A | | C,A | | C,I | | C,I | | C,I | | C,A | |

1. Email data

|  |  |  |
| --- | --- | --- |
| Asset | Threats | CIA? |
| E.g. Email Data | |  | | --- | | Server Failure | | Hacking | | Malware | | Employee Misuse | | Employee Thief | | SQL Injection | | |  | | --- | | C,A | | C,A | | C,A | | C,I | | C,A | | C,I | |

1. Employee Data

|  |  |  |
| --- | --- | --- |
| Asset | Threats | CIA? |
| E.g. Employee Data | |  | | --- | | Employee Thief | | Phishing | | Malware or Ransomware | | Social Media Attack | | Mobile Malware | | Unauthorized Access | | Men-in-the-Middle-Attack | | |  | | --- | | C,A | | C,I | | C,A | | C | | C,A | | I | | C,A | |

1. E-Auction Side Information

|  |  |  |
| --- | --- | --- |
| Asset | Threats | CIA? |
| E.g. Side Information | |  | | --- | | Employee Thief | | Phishing | | Malware or Ransomware | | Social Media Attack | | Mobile Malware | | Computer Worm | | Unauthorized Access | | Adware and Spyware | | Rootkit | | |  | | --- | | C,A | | C,I | | C,A | | C | | C,A | | C | | I,A | | C,A | | C,A | |

1. Likelihood and Impact
2. Bidding Side Information

|  |  |  |
| --- | --- | --- |
| Threats | Likelihood | Impact |
| Employee Thief | High | High |
| Server Failure | Low | Medium |
| Environment Risk | Medium | High |
| Hacked | Medium | High |
| Spyware | Medium | Medium |
| Unauthorized Access | Low | Low |
| DDOS Attack | Low | Low |
| Phishing | Medium | Medium |
| SQL Injection | Medium | Medium |
| Men-in-the-Middle-Attack | High | High |

1. Personal Information

|  |  |  |
| --- | --- | --- |
| Threats | Likelihood | Impact |
| Server Failure | Low | Medium |
| Malware or Ransomware | Medium | High |
| Social Media Attack | Medium | Low |
| Employee Thief | High | High |
| Mobile Malware | Medium | Medium |
| Unauthorized Access | Low | Low |
| Computer Virus | Medium | Medium |
| Phishing | Medium | Medium |
| SQL Injection | Medium | Medium |
| Man-in-the-Middle-Attack | High | High |

1. Email Data

|  |  |  |
| --- | --- | --- |
| Threats | Likelihood | Impact |
| Server Failure | Low | Medium |
| Hacking | Medium | High |
| Malware | Medium | Medium |
| Employee Misuse | Medium | Low |
| Employee Thief | High | High |
| SQL Injection | Medium | Medium |

1. Employee Data

|  |  |  |
| --- | --- | --- |
| Threats | Likelihood | Impact |
| Employee Thief | High | High |
| Phishing | Medium | Medium |
| Malware or Ransomware | Medium | Medium |
| Social Media Attack | Medium | Low |
| Mobile Malware | Medium | Medium |
| Men-in-the-Middle-Attack | High | High |

1. E-Auction Side Information

|  |  |  |
| --- | --- | --- |
| Threats | Likelihood | Impact |
| Employee Thief | High | High |
| Phishing | Medium | Medium |
| Malware or Ransomware | Medium | Medium |
| Social Media Attack | Medium | Low |
| Mobile Malware | Medium | Low |
| Computer Worm | Medium | Medium |
| Adware and Spyware | Medium | Medium |
| Rootkit | High | Medium |

1. Risk Matrix
2. Bidding Side Information

|  |  |
| --- | --- |
| Threats | Risk |
| Employee Thief | Very High |
| Server Failure | Low |
| Environment Risk | High |
| Hacked | High |
| Spyware | Medium |
| DDOS Attack | Very Low |
| Phishing | Medium |
| SQL Injection | Medium |
| Men-in-the-Middle-Attack | Very High |

1. Personal Information

|  |  |
| --- | --- |
| Threats | Risk |
| Server Failure | Low |
| Malware or Ransomware | High |
| Social Media Attack | Low |
| Employee Thief | Very High |
| Mobile Malware | Medium |
| Unauthorized Access | Very Low |
| Computer Virus | Medium |
| Phishing | Medium |
| SQL Injection | Medium |
| Man-in-the-Middle-Attack | Very High |

1. Email Data

|  |  |
| --- | --- |
| Threats | Risk |
| Server Failure | Low |
| Hacking | High |
| Malware | Medium |
| Employee Misuse | Low |
| Employee Thief | Very High |
| SQL Injection | Medium |

1. Employee Data

|  |  |
| --- | --- |
| Threats | Risk |
| Employee Thief | Very High |
| Phishing | Medium |
| Malware or Ransomware | Medium |
| Social Media Attack | Low |
| Mobile Malware | Medium |
| Men-in-the-Middle-Attack | High |

1. E-Auction Side Information

|  |  |
| --- | --- |
| Threats | Risk |
| Employee Thief | Very High |
| Phishing | Medium |
| Malware or Ransomware | Medium |
| Social Media Attack | Low |
| Mobile Malware | Low |
| Computer Worm | Medium |
| Adware and Spyware | Medium |
| Rootkit | High |

Task 2

Controlling the Risk

# Task (2) Controlling the Risk

1. Threats
2. Server Failure

There has many risks to failure the Server. If server go down, the business data important data can lose. Then lost hardware breakdown, device errors, network partitions and unexpected client activity will all lead to server instance failure. One of the factor of server break down is overheating. All the electricity used in a server room is turned into heat. When the server run time is too long, server room temperature is started rise. Sometime server can burn and can lose the important data. Then the most common failure issues is virus attack. When server is connect to the company’s website, there can virus through the website and reach the server and the important data must be stolen or damage.

Not to rise the server room temperature, we should make a cooling feature in the server room. During the cooling feature, the IT experts recommend keep server in the temperatures between 55 and 72 degrees Fahrenheit. Then dust and dirt will built up in easily so keep cleaning the server room. For virus attack, using the web filtering software. In scenario, company need a web filtering software and the server room can be more secure.

(Anon., n.d.) (Anon., n.d.)

1. Employee Thief

Employee thief is a considerable problem for many companies. It defines as any stealing, use or use of employer’s assets without permission. There are many reasons for normally stealing such as

(Anon., n.d.) (Anon., n.d.)

1. Environmental Risk

The most common Environmental risk are server room temperature, room moisture, leaking of water, human mistake, and noise and power outage. One of the human mistake is forgetting to reset the adjusting to heat or air condition when they leave the server room. And natural environmental threats such as earthquake and floats.

In this environmental risk, server room can prevent from the human error such as forgot to adjust the room temperature and forgot the check the room. But the natural risks such as earthquake and floats are not easy to prevent from these threats. To prevent this risk, company can set up a backup server

(Anon., n.d.) (Anon., n.d.)

1. Hacked

Hacking are constantly looking for the way to crack into the computer networks. Hacker through the company security system for many purposes. Hacking involves a variety of forms, such as breaking the password and injecting the virus into the social engineering environment where the network administrator is located. Hacking is challenge for a business security system and it is need to prevent and reduce the possibility of a system being hacked.

To prevent from hack, company need to use a strong password policies. Passwords should have at least eight safe characters, a mixture of combinations of alpha and numeric characters, and top and bottom letters. And then they should use a web filtering software and rent a cyber-security team to manage the computer network security and prevent from hacking.

(Anon., n.d.)

1. Malware or Ransomware(Spyware)

Spyware is a software that is infiltrates the computer device and stealing the internet usage data and sensitive business information. Spyware is a type of malware. Malware is a software it is design to gain access to or damage the computer. Spyware is used for many purposes such as track and steal the personal information. It can monitoring the internet activity, tracking the login and password information. It can receive from the downloading software form the unknowing website and opening email attachments from unknown sender.

Spyware can damage the data but it can be prevent by using an antivirus tools.

(Anon., n.d.)

1. DDOS Attack

Distributed denial-of-service attack (DDOS Attack) is a way of cyber security attack that is target to attack the website and online services. The aim of the DDOS attack is to overload them with more traffic than could be accommodated by the server or network. The purpose of this is to make the website or service inoperable.

To prevent the DDOS, company should need to configure the hardware in network against attacks and to protect the domain name system (DNS) server.

(Anon., n.d.) (Anon., n.d.)

1. Phishing

Phishing is the type of social engineering attack and using it for stealing the company information. Phishing techniques are Email Phishing and Spear Phishing. In email phishing, an attacker sending a thousand of fraudulent message for network traffic. Spear phishing is an email or electronic communication scheme targeted at a specific person, organization or business.

For prevent from phishing, using Two-factor authentication (2FA) and it is the most effective method for the countering phishing attacks. And avoid using public network and safely handle that is to manage to research user.

(Anon., n.d.) (Anon., n.d.)

1. SQL Injection

An SQL injection is a type of cyber-attack in which a hacker used a piece of SQL code to manipulate a database and gain access to the potentially valuable information.

There are several way to prevent the SQL injection. There are using a firewall for a web application. And another prevention is the database user account is only specific and trusted people can access the database.

(Anon., n.d.)

1. Man-in-the-Middle-Attack

Man-in-the-Middle attack are the common type of cybersecurity attack that allow the attacker to track the contact between two targets.

Brest way of prevention man-in-the-middle attack are using strong WEP/WAP Encryption on the access point, using virtual private network and public key pair based authentication.

(Anon., n.d.)

1. Rootkit

Rootkit is a covert programing program designed to provide continued access to a computer while actively hiding its presence. A rootkit can allow to someone to maintain command and control over a computer without user or owner knowing about it.

Rootkit are so dangerous and difficult to detect it. To prevent the rootkit, check the computer’s application and operation system. And checking the phishing email and be careful the downloading by drive.

(Anon., n.d.)

## Encryption and Protocol

Encryption is a way to scramble data that only authorized parties can understand the information In terms of technology. In Smith and Jones has many auction sides more than 60. So Smith and Jones should need to secure when they transport the data one side to another and need to use encryption. Encryption can help the data breaches, whether it is in transit or at rest. (Anon., n.d.)

In this encryption algorithm will be used. For store data, EFS (encryption file system) will be use because there has strong encryption security key.

For transmit data, company should used VPN. In this VPN Layer 2 Tunneling Protocol (L2TP) should be use. It prevent data from being altered while moving between sender and receiver. (Anon., n.d.)

For Wi-Fi, Wi-Fi protected access 2 (WPA2) will used for this company. These has use strong encryption. (Anon., n.d.)

Task (3)

Setting up the VPN

# Task (3) Setting up the VPN

## Intranet and Extranet

## Difference of Intranet and Extranet

**Intranet** is a private computer network that is used the internet protocol, network access and probably the telecommunication system to secure share part of organization’s information or operation operations with its employee.

**Extranet** is an intranet that can be accessed partially by registered local users allowing company to share information secure over the internet. It is manage private network that provide access to the partner, and approve group of customers usually to a subset of information that can be access form a company’s intranet. (Anon., n.d.)

### Benefit of Intranet

* Help improve the internal communication
* High impact corporate communication
* Improve Employee engagement
* Corporate Memory and Knowledge Sharing
* More Improve customer services

(Anon., n.d.) (Anon., n.d.)

### Benefit of Extranet

* Increased productivity
* Reduce Margin of error
* Information sharing is simple
* Document are safe and secure
* Easily management to project
* Simple setup and maintenance

(Anon., n.d.) (Anon., n.d.)

### Recommendation

Both Intranet and extranet offer centralized data storage and collaborative tools. In intranet and extranet, extranet is more creates a collaboration space not only for employee but also for customer. Intranet only allow employee to use the system. In extranet, it is open up access for external company user. The data and contact are store in the intranet is only available for the internal user. However, in the extranet, the store data is for both internal and external user. Both intranet and extranet depending on the type of platform that is used and, both system can offer the same type of features and contact. In Smith and Jones, there has more than 60 auction sites and they transport the data from one site to another. Intranet is good but it can available for one site. Extranet are accessible from outside the network. In this extranet, user can corporate intranet from home and it can connect with a secure connection to within the computer intranet. In the extranet, the intranet system is already involve and more secure than intranet. So extranet is most suitable for this company.

(Anon., n.d.) (Anon., n.d.)

## Network Diagram



# Rule of Firewall

### VPN Security Feature Lists

* Automatic unsecure Wi-Fi protection
* DNS Leak Protection
* IPv6 Leak Protection
* Kill Switch
* Strong Protocol
* Strong Encryption
* Connection Obfuscation

(Anon., n.d.)

### Why Firewall needed?

Firewall is a barrier or shield that is intended to protect the data form the database malware danger that is exist on the internet. Data is exchanged between computer and server and router in cyberspace and firewall is monitor this data to check the data is safe or not. Most operation system feature built-in firewall. Firewall is used for control access, server implementation, monitoring and alerting, protect the local network and virus protection form the other.

Firewall can protect the data from the unauthorized remote access. In the scenario, need to prevent and reduce the employees or customers click link to the unknown access. In this part, firewall is important for this problem.

Firewall can manage and block the messages linking to unwanted contact and it can manage the data input output etc. So strong firewall is making a great security for this company.

(Anon., n.d.) (Anon., n.d.)

### Rule of Firewall

A firewall rule consists of firewall service, which define the type of traffic and ports used for that type of traffic. Firewall rule are an important part of the network security. Firewall rule for this company is –

* Keep Firewall always turn on.
* Updating to the last version of Firewall.
* Monitor user access to the firewall setting.
* Block the suspicious link to circumvent the company firewall.
* Instill the process of testing and auditing the firewall that will help for the firewall security.
* Updating latest version of operation system for the firewall.

(Anon., n.d.) (Anon., n.d.)

Task (4)

Maintaining Security

# Task (4) Maintaining Security

For the company security, the company should pay the training for their employee about the maintaining security. Company explain the employees and customers not to click the unknown link. The make the security policy for the employee. These policies are use password is strong and unique with employee account and separate the role of employee. And keep personal and Bidding Side Information secure. According to the role of employee, their authority is limited. Setting up the CCTV in the workplace area.

Training the employee to avoid opening the suspicious-looking email and not to click the link. And installing the antivirus software and set it to automatically update. Run the latest version of the software and careful there must be up to date. Training the employee, how to prevent unauthorized access to the Email information. And update the security level to prevent from the employee thief and hacker access to gain the sensitive information.

Task (5)

# Task (5)

## Problem and Solving

In this Task (1) and Task (2), there has a problem to research the cyber security threats. There has many security threats but these all of threats are similar another threats. So prevention way are the same and so recommendation for the prevention ways are the same. So there has a few words for the recommendation for a threats. In recommendation of encryption and protocol, there has a problem to choosing them. These two have their related benefit. So it is difficult to select the one. In Task (3), I have weakness in the network security. In this, searching the intranet and extranet, these two services are the same benefit and a little differences things. Then in drawing network diagram, I have not a software for the diagram and lack a knowledge of how to draw the diagram. And searching problem in the firewall features. In searching firewall features, the result is outputting the ACL features. Their feature like the same but they are different.

For prevention, in searching threats, collect the similar threats and recommend the prevention ways. And choosing the encryption protocol because there has some protocol in this service. For the VPN and network diagram, searching and learning form the online. For the firewall rules, asking some people and searching online and solve it.

## When I start again

If I have a chance to have start again this assignment, using cloud service for the store data. It is reduce the transport service and all of sits can connect the cloud. And company will used VPN in firewall, router and swift. If I chance to start it again, I want to make better than above factor.

# References

# Bibliography

Anon., n.d. [Online]   
Available at: https://www.lawinsider.com/dictionary/business-infprmation

Anon., n.d. [Online]   
Available at: https:///simplicable.com/new/business-data

Anon., n.d. [Online]   
Available at: https://smasllbiztrends.com/2018/10/personal-information.html

Anon., n.d. [Online]   
Available at: https://legalvision.com.au/q-and-a/what-can-be-considered-confidential-information/

Anon., n.d. [Online]   
Available at: https://www.bitsight.com/blog/sensitive-data-example-how-to-protect-it

Anon., n.d. [Online]   
Available at: https://docs.oracle.com/cd/E13222\_01/wls/docs90/server\_start/failures.html

Anon., n.d. [Online]   
Available at: https://download.schneider-electric.com/files?p\_Doc\_Ref=SPD\_DBOY-7CDJNW\_EN

Anon., n.d. [Online]   
Available at: https://www.inc.com/encyclopedia/employee-theft.html

Anon., n.d. [Online]   
Available at: https://businesspracticalknowledge.wordpress.com/legal-security/employee-theft/

Anon., n.d. [Online]   
Available at: https://www.ieci.com.au/applications/wp-enviro-mon.pdf

Anon., n.d. [Online]   
Available at: https://blog.storagecraft.com/top-5-data-center-environmental-standards-and-concerns/

Anon., n.d. [Online]   
Available at: https://blog.storagecraft.com/top-5-data-center-environmental-standards-and-concerns/

Anon., n.d. [Online]   
Available at: https://yourbusiness.azcentral.com/prevent-hackers-company-23336.html

Anon., n.d. [Online]   
Available at: https://www.imperva.com/learn/application-security/phishing-attack-scam/

Anon., n.d. [Online]   
Available at: https://usa.kaspersky.com/resource-center/definitions/spear-phishing

Anon., n.d. [Online]   
Available at: https://www.kaspersky.com.au/resource-center/definitions/sql-injection

Anon., n.d. [Online]   
Available at: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

Anon., n.d. [Online]   
Available at: https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html

Anon., n.d. [Online]   
Available at: https://www.cloudflare.com/learning/ssl/what-is-encryption/

Anon., n.d. [Online]   
Available at: https://medium.com/@stangarfield/what-is-the-difference-between-the-internet-an-intranet-and-an-extranet-a86c0765ecfe

Anon., n.d. [Online]   
Available at: https://blog.jostle.me/blog/benefits-of-an-intranet

Anon., n.d. [Online]   
Available at: https://www.jivesoftware.com/blog/benefits-of-intranet/

Anon., n.d. [Online]   
Available at: https://www.allbusiness.com/the-benefits-of-an-extranet-1283-1.html

Anon., n.d. [Online]   
Available at: https://www.glasscubes.com/five-reasons-why-your-business-needs-an-extranet/

Anon., n.d. [Online]   
Available at: https://www.cmswire.com/digital-workplace/intranets-vs-extranets-why-you-need-both/

Anon., n.d. [Online]   
Available at: https://smallbusiness.chron.com/extranet-vs-intranet-company-use-11878.html

Anon., n.d. [Online]   
Available at: https://pixelprivacy.com/vpn/vpn-security-features/

Anon., n.d. [Online]   
Available at: https://www.makeuseof.com/tag/5-reasons-use-firewall/

Anon., n.d. [Online]   
Available at: https://cos.reis.ca/blog/why-does-my-business-need-a-firewall

Anon., n.d. [Online]   
Available at: https://www.secpoint.com/top-10-tips-for-using-a-firewall.html

Anon., n.d. [Online]   
Available at: https://help.f-secure.com/product.html#business/client-security/13.00/en/concept\_F980D184D74D4FF0A79562231548178C-13.00-en

Anon., n.d. [Online]   
Available at: https://www.google.com/amp/s/vpn-services.net/advantageous-and-disadvantageous

Anon., n.d. [Online]   
Available at: https:/www.summitdata.com.blog

Anon., n.d. *esecurityplanet.* [Online]   
Available at: https://www.esecurityplanet.com/network-security/how-to-prevent-ddos-attacks.html

Anon., n.d. *norton.* [Online]   
Available at: https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html

Anon., n.d. *norton.* [Online]   
Available at: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html

# Candidate Checklist

Please use the following checklist to ensure that your work is ready for submission.



Have you read the NCC Education documents 'What is Academic Misconduct? Guidance for Candidates' and 'Avoiding Plagiarism and Collusion: Guidance for Candidates' and ensured that you have acknowledge all the sources that you have used in your work?



Have you completed the 'Statement and Confirmation of Own Work' form and attached it to your assignment? **You must do this**.

Have you ensured that your work has not gone over or under the recommended word count by more than 10%?



Have you ensured that your work does not contain viruses and can be run directly?

